International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 3, Issue 5, Dec 2013, 129-138

ROUTING SCHEME DEVELOPMENT FOR FIREWALL SECURITY IN WIRELESS AD HOC NETWORK USING ELECTION ALGORITHM

PURNIMA[1] & AMAN SINGH[2]

[1]Assistant Professor, Innocent Heart Institution, Jalandhar, Punjab, India

[2]Assistant Professor, Lovely Professional University, Phagwara, Punjab, India

ABSTRACT

MANET stands for mobile adhoc network. In MANET the infrastructure is dynamic, self configured and self-governed. This can be used for various purposes. It can be created in emergency conditions or can be created on the basis of user's needs and requirements. No fixed topology can be defined in this type of network. Various kinds of threats increase the vulnerability of MANET. Attacks like black hole are commonly found in this kind of network. MANET is highly prone to security issues due to its vulnerabilities. These issues can be handled in different ways. In this paper solution as Intrusion detection system (IDS) is implemented with an attack finder protocol via taking Election algorithm as the main area for defending black hole attack.

KEYWORDS: MANET, Ad-Hoc Network, Firewall, Simulation, Self-Configuring, IDS, Election Algorithm

INTRODUCTION

The use of wireless network has grown exponentially with the emergence of wireless devices. A great advancement in network infrastructure has also been seen in the last decade along with the growing availability of wireless applications. The needs of vastly growing independent mobile users are continuously increasing the number of wireless communication system in next generation.

There are two kind of wireless networks one is Infrastructure network and other is Wireless Ad- hoc network. Wireless Ad-hoc networks are those networks in which nodes are self-managed, self-organized and self-governed. There is no infrastructure for these kinds of nodes. Nodes can easily join and leave the network at any time. In Ad-hoc network, devices act themselves like the network.

Mobile Ad-hoc network is different from other network solutions. Users can create their own network and can deploy them easily and cheaply. Their transmission range is small. Every node in MANET is considered as a router. It discovers a path to forward the packets to right node in the network. As the nodes are free to move router organize them randomly. In MANET network topology is dynamic due to which constraints like battery power, bandwidth and security make the design of sufficient protocols as a major challenge.

In this paper challenging features of MANET are discussed. In MANET security constraints are the major issues in which lot of attacks can breach the security. Black hole attack is one of them. Hence any approach designed for the security mechanism of a system resembles an attack like Black hole attack that is faced by the system and given vulnerabilities. This approach should ensure that the network is secured with these attacks and vulnerabilities.

To implement security in MANET, the information of services like security against attacks and protection of nodes is necessary. These services can be categorized in two types, one is Communication Security and other is Computer Security. Communication security is the protection against active and passive attacks. On the other hand, the computer

security can be implemented at hardware and software basis. This paper is based on the investigations of the communication security development in MANET on software basis.

This paper presents Literature Review in section II. Black hole is written in the section III. Section IV illustrates new proposed approach. Section V shows result and discussion. And at the end future work and conclusions are presented**.**

LITERATURE REVIEW

Jian-zhu and Jipeng Zhou [1] have proposed efficient authentication mechanisms for low-power devices. In their proposed scheme, the mobile station only needs to pass one packet for mutual authentication. They used the elliptic-curve-crypto system based on trust delegation mechanism to generate pass code for mobile station authentication. With the use of this authentication mechanism, many active and passive attacks were prevented including the denial of service attack. The mobile device was authenticated with the visiting base station only by the exchange of one packet. This proposed mechanism required less computations and less message exchange as compared to other authentication schemes [4].

Tier-ho Chen et al., has highlighted the importance of the mutual authentication for wireless sensor networks. They have also presented the DAS protocol which is hash-based authentication protocol, and provides the security against the replay, masquerade and guessing attacks. The weaknesses of the DAS protocol were also discussed in their study where they have proposed enhancements in the DAS protocol. The enhanced DAS protocol is efficient than the traditional DAS protocol. Enhanced DAS protocol is reliable protocol and provides more security to the sensor nodes in the insecure environment. The proposed protocol is the energy efficient protocol and require less message exchange and less computations for mutual authentication (2010) [3].

Sushma yalamanchikiand et al. have proposed a two Stage authentication scheme for wireless networks. They discussed that the wired network can use the authentication protocol with large computations but wireless networks require less computation and energy efficient authentication protocol. Because in wireless networks the hand held devices have limited battery and computational resources and it also suffers from packet losses, bit errors and low bandwidth. They have presented 2-stage authentication scheme for wireless networks. It uses a computationally intensive and highly secure strong authentication in Stage 1 and a lightweight symmetric key based protocol in Stage 2. The cost of the strong authentication adopted in Stage 1 is amortized over N sessions thus reducing the overall cost of the scheme. It adapts the Dual-signature based IKE authentication which they had proposed in their earlier work and they have employed it as Stage 1 authentication. The Symmetric key protocol in Stage 2 authentication that they proposed uses the symmetric keys that are generated in Stage 1[5].

P. Chatzimisios et al. (2004) [6] have focused on RTS/CTS reservation The effectiveness of the RTS/CTS reservation scheme is examined in reducing the collision duration for IEEE 802.11a DCF. They studied this work for impact of using the RTS/CTS scheme in high data rate WLANs and for different data and control transmission rates without the presence of hidden stations. They conclude that the overall WLAN performance suffers significantly when the lower rate RTS/CTS exchange reservation scheme is combined with higher transmission data rates. The RTS scheme has disadvantage for high data rates and small network scenarios and its effectiveness in improving performance is uncertain.

Govind Sharma et al. (2012) [4] have proposed an approach to detect the black hole attack in Mobile Ad-hoc network. Their approach is based on AODV (ad-hoc on demand distance vector) routing algorithm. They have enhanced the secured AODV routing algorithm by using promiscuous mode of the node that can learn about the neighboring routes traversed by data packets, if operated in the promiscuous mode. They have provided a feasible solution to detect the black hole attack.

Anu bala et al. (2009) [2], have focused on black hole attack which is the one of the possible attack of mobile ad hoc network. They have used a network simulator tool NS2 to define the concept of black hole in which they analyze that the packet loss increased in the network with black hole node. They have also observed that the throughput have decreased and end to end delay have increased in the network with a black hole node.

Sandipan basu et al. have presented election algorithm that can be used in distributed systems to elect a coordinator and choose the head. This is an enhanced version of an already existing election algorithm that is also called a bully algorithm, developed in 1982. They proposed an algorithm which is efficient in terms of number of messages needed to perform an election and recovery of a failed process, as compared to the Bully Algorithm. (BASU)[7].

BLACKHOLEATTACK

Black hole attack (see figure 1) is one of the denials of service (DOS) attacks which is studied in this paper. In this attack malicious node may drop all packets that it receives for forwarding. Special effect of this attack can be seen when black hole node is specially a sink hole. This combination can stop all data traffic around the black hole. In this attack malicious node uses its protocol to advertise itself for having shortest path to the destination.

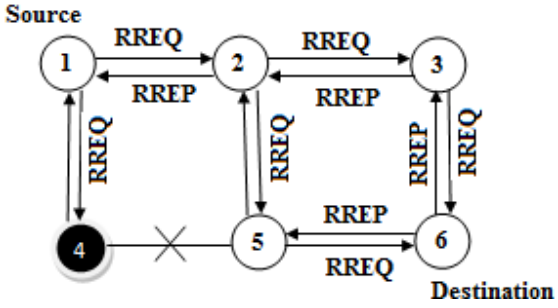

Figure 1: Blackhole Attack

Malicious node's reply is always available for the request of route. Before the reception of reply from actual node, a forged route is created. After linking with malicious node it is up to the node weather to forward the packet to unknown address or drop all the packets.

PROPOSED APPROACH

The proposed approach in this paper is to implement IDS based on election algorithm. Efficient route for the packets using algorithm is found (Adhoc on demand attack detection distance vector routing protocol (AOADDV) routing protocol scheme generate) so that prevention from black hole can be done and throughput and end to end delay is revoked out and performance is enhanced.

An algorithm is implemented in which every node has to present its resources to their corresponding nodes. The node which has higher resources is selected as head. Every head in network maintains a table, which is responsible for data routing. When a head receives data from the corresponding head it checks and filters the coming data if it belongs to malicious nodes packet.

In MANET every node can act as a head or a central controller because of its properties. A firewall is generally implemented on the central controller. It can be embedded on the head also. The head is then responsible for packet filtering. In the present work architecture firewall works only on the MPR using AOADDV protocol that filters the incoming and outgoing untrusted traffic.

Election Algorithm to detect black hole attack

Terminology (EVENT Node "S" have data for "D")

Notations:

S: Source Node, D: Destination Node

Routing table, link table, NB set, NB2 hope set, MPRsel set, Topology set, originator address, AOADDV_checking message, Unicast_RREP, AOADDV_Mid Message.

S Send RREQ;

/* Start to search the Route for

Destination */

Initialise_ timer_T_RREQ;

/* Timer, for checking Route Reply time out */

AOADDV_CHECKING_INTERVAL=2, AOADDV_MID_INTERVAL=5, AOADDV_UNICAST_RREP=5.

Destination flag=false;

Create MPR selector set for each interface using two subsets like N, N2 [9].

/*N is the set of 1-hop neighbour*/.

/*N2 is the set of 2-hop neighbour*/

Compute routing table for all nodes .like link table, interface table, and topology table.

Repeat next step

While (destination_flag==false*)*

Send %AOADDV message

/* which update MPR selector set*/

Send Uni-Cast RREP

/* which updates topology table*/

Send Mid-Massage

/ which update interface table/

Update routing table on the basis of previous updation on MPR Selector set, topology table and interface table.

If (routing table updated)

Set Destination_flag= true

End if

Exit

AOADDV is working as the proactive routing protocol because in this routes are available as and when required. It works on a pure link state protocol as change in the topology causes the flooding of the topological information to all available nodes in the network. We use multipoint relay (MPR) to reduce the possible overheads in the network. The basic function of MPR is to reduce flooding of broadcast messages by reducing the same in some region of the network.

AOADDV use two kinds of control messages one is AOADDV_CHECKING message and another is AOADDV_UNICAST_RREP. MID message intervenes when two interfaces occur in AOADDV_UNICAST_RREP.

AOADDV_CHECKING messages help in finding the information of link status and the neighbor of the node. MPR selector set is constructed with the hello message that describes which neighbor node has to be chosen.This node acts as a MPR. Hence, from this information the node can calculate its own set of MPR's.AOADDV_CHECKING messages are sent only one hop away at an interval of 2 microseconds. Therefore they are not forwarded any further.

AOADDV_UNICAST_RREP messages are broadcasted throughout the entire network. These massages provide broadcasting information about their neighbours which include the MPR selector list. These messages are broadcasted at an INTERVAL of 5 microseconds and can be forwarded only by the MPR nodes. There is also multiple interface declaration (MID) AOADDV_MID_MEASSAGES which provide information to other nodes that the announcing node can have multiple interface addresses. AOADDV_MID_MEASSAGES are broadcasted throughout the entire network by MPR selector.

In AOADDV_CHECKING when the first node receives the AOADDV_CHECKING message from the second node it sets the second node's status as asymmetric in the routing table. When the first node sends an AOADDV_CHECKING message to the second node and ensures that it is asymmetric. The second node in turn sets the first node's status as symmetric on routing table. Finally when second node send a AOADDV_CHECKING message again where the status of the link for the first node is indicated as symmetric then first node changes the status from asymmetric to symmetric. AOADDV_CHECKING messages provide information about local links and AOADDV_CHECKING neighbours. The AOADDV_CHECKING message are used for link sensing ,neighbor detection and MPR selection process .This message contains information how often the nodes sense the AOADDV_CHECKING message , willingness of node to act as the MPR and information about its neighbor like interface address, link type and neighbor type.Which may forward its message? Each node has information about the symmetric one hop (N) and two hop (N2) neighbours in order to calculate optimal MPR set. Information about the neighbours is taken from the AOADDV_CHECKING message. The two hop neighbours found from AOADDV_CHECKING because each AOADDV_CHECKING message contains all the information about the neighbor nodes. MPR selection is done on the basis of highest Willingness of the nodes if two or more nodes have the same willingness then it picks a node with maximum degree.

When the host gets a new broadcast message, which is to be spread in the network and message sender interface address is in the MPR selector set, then the host must forward the message. The MPR selector set is continuously updated using AOADDV_CHECKING messages.

Flow Chart of Proposed Architecture

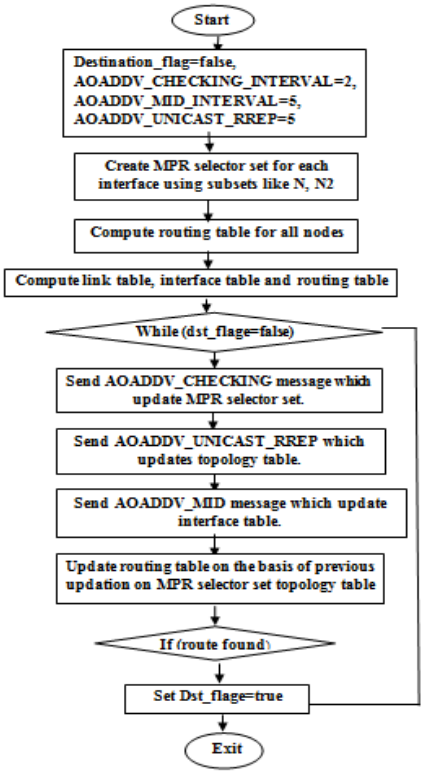

Figure 2: Proposed Architecture

Flow Chart of MPR Selection Set

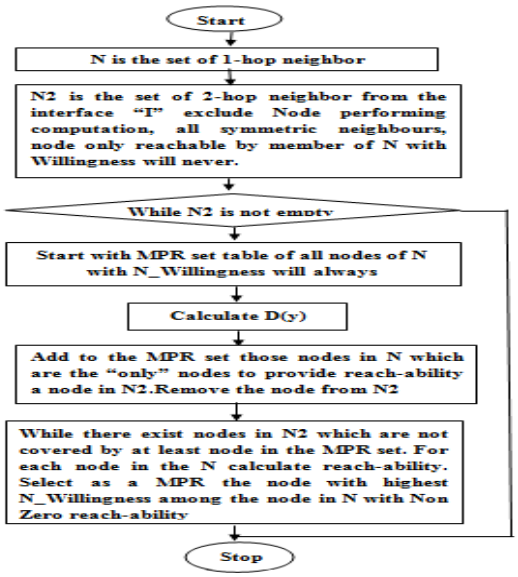

Figure 3: MPR Selection Set

The above flow chart describes the selection of MPR selection set. MPR set is constructed with minimum number of 1-hop symmetric neighbor (N). Hence, it is possible to reach all 2-hop symmetric neighbours (N2), excluding nodes performing computation, all symmetric neighbor nodes, and nodes only reachable by member of N with willingness will never, till N2 is not empty. MPR selection set is then constructed with all member nodes of N with N_Willingness. Only those nodes of N are added to MPR set that provide reachability to N2, rest of the N2 nodes are removed. If still, any node exists in N2 which is not covered by the least node in MPR set N will again calculate the reachability. Node with highest

willingness with N will be selected. If two or more nodes have the same willingness then it picks a node with maximum degree.

Elected MPR needs to send AOADDV_Unicast_RREP message which is broadcasted in network by MPR periodically. This message advertises its own link in the network. It contains sequence number of messages. This sequence number is used for the freshness of message .If the node gets a message with smaller sequence number, message is discarded without any updation. Sequence number is incremented in two cases. First, when links are removed from AOADDV_Unicast_RREP message and second, when links are added to the message

Flow Chart of Routing Table

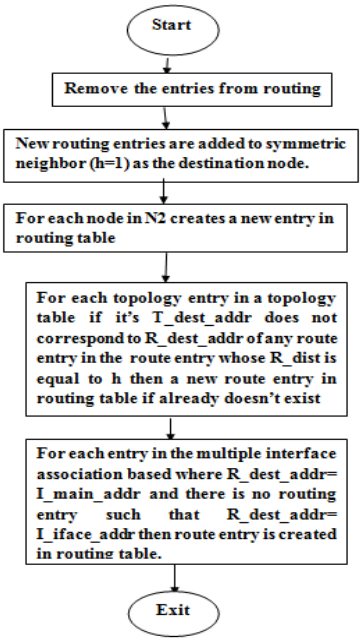

Figure 4: Routing Table Calculation

The above flow chart shows that the nodes maintain the routing table. Routing table fields include Destination address, Number of hops to the destination, Local interface address, and Next address. This address indicates the next hop address. Information is taken from AOADDV_Unicast_RREP message and AOADDV_CONTROL message. If any change occurs in these two messages then routing table will be updated. No information about the broken links is stored in this table.

Changes can occur in the routing table due to the appearance or disappearance of neighbor link, creation or removal of 2-hop neighbor is also responsible for a change in routing table, change cal also be seen when Topological linkappears or lost or due to MID message information change.

Simulation and Result

In this study NS2 simulator has been used [8]. NS2 is a network simulation tool that simulate wired and wireless node communication network. NS2 provides a comprehensive environment for designing network protocols. It creates and visualizes scenario under specific condition and analyzes their performance.

In the presented simulations, CBR (Constant Bit Rate) application, TCP/IP, IEEE 802.11 MAC and wireless channel based on Tworayground propagation model have been used (see figures 2 - 4). The simulated network consists of

52 random allocated wireless nodes in a 500 by 500 square meter flat space.A traffic generator was developed to simulate constant bit rate (CBR) sources.

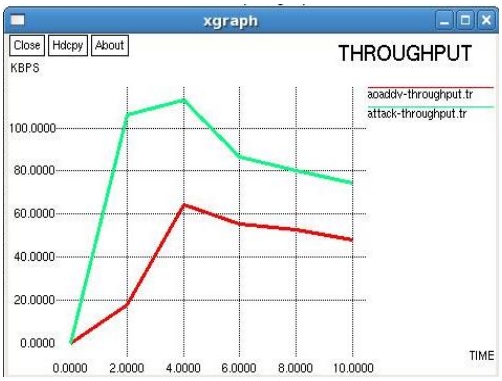

Figure 5: AOADDV Throughput and Attack Throughput

Figure 6: AOADDV Delay and Attackthroughput

Figure 7: AOADDV Packet Delivery Ratio and Attack PDR

In above figure 5, 6.and 7 shows the graphs of throughput, packet delivery ratio and average delay .packet loss due to black hole attack, bottleneck problem, queue size congestion and malicious packet. Figure 5 shows the throughput and throughput basically defined as a ratio of the number of bits recived over the time different between first and last reciving packet. In figure 6red lines shows AOADDVthroughput and green line shows throughput after prevention of attack. In figure 6 shows average delay or end to end delay and end to end delay of packet is defined as the time a packet takes to travel from source to the destination. And in figure 6 red line shows AOADDV delay and green line shows delay after prevntion of attack. In figure 7 shows packet delivery ratio and PDR defined as ratio of the number of packet actulaly

recived over the number of data packet transmitted by the sender. And in figure 7 red line shows AOADDV PDR and green line showsAOADDV PDR and green line shows PDR aftre prevention of attack.

CONCLUSIONS

In this paper, it is concluded that the packet filtering is important in every network to prevent various types of attacks. In this study packet filtering is implemented through the use of the Election Based Algorithm IDS System on MANET. In different types of networks, there are different methods to apply packet filtering, such as it is very easy to implement in the centralized network, but it is too complicated in the self configure type of network that is ad hoc network. This is because in ad hoc network there is no central controller and in addition it has a unique feature of self configuring. In this work the requirements are gather to implement election algorithm based firewall in mobile ad hoc network. It also highlights the advantages of IDS. The election algorithm based filtering technique is based on efficient routing in which black hole is detected.

FUTURE WORK

A new algorithm could be derived to filter the packets with enhanced Throughput, Energy Efficiency and End to End Delay. A new mechanism can also be developed for saving drop packet due to malicious nodes so that retransmission of a packet can be reduced. In future an efficient technique can also be evaluated on the basis of which we choose a controller.

REFERENCES

1. Jian-zhu Lu and Jipeng Zhou.” On the Security of an Efficient Mobile Authentication Scheme for Wireless Networks”
2. Anu Bala, Munish Bansal” performane analysis of MANET under black hole attack”
3. Tien-Ho Chen and Wei-Kuan Shih.” A Robust Mutual Authentication Protocol for Wireless Sensor Networks”
4. Govind Sharma, M. G.” Black Hole Detection in MANET Using AODV Routing Protocol”.
5. Sushma Yalamanchiliand K. V. Sambasiva Rao.” TWO-STAGE AUTHENTICATION FOR WIRELESS NETWORKS USING DUAL SIGNATURE AND SYMMETRIC KEY PROTOCOL”
6. P. Chatzimisios, A.C. Boucouvalas et al” Effectiveness of RTS=CTS handshake in IEEE 802.11a Wireless LANs”
7. Sandipan basu” An Efficient Approach of Election Algorithm in Distributed Systems”
8. NS-2, "Network simulator 2 (NS2), http://www.isi.edu/nsnam/ns/," in NS, 2008.
9. “Internet engineering task force, http://www.ietf.org/rfc/rfc3626.txt